11-28-2018

An Experiment Series on App Information Privacy Concerns

Christoph Buck
University of Bayreuth, christoph.buck@uni-bayreuth.de

Simone Burster
University of Bayreuth, simone.burster@fim-rc.de

Torsten Eymann
University of Bayreuth, torsten.eymann@uni-bayreuth.de

AN EXPERIMENT SERIES ON APP INFORMATION PRIVACY CONCERNS

Research paper

Buck, Christoph, University of Bayreuth, Bayreuth, Germany, christoph.buck@uni-bayreuth.de

Burster, Simone, University of Bayreuth, Bayreuth, Germany, simone.burster@uni-bayreuth.de

Eymann, Torsten, University of Bayreuth, Bayreuth, Germany, torsten.eymann@uni-bayreuth.de

Abstract

The diffusion of smart mobile devices and therewith apps into everyday life comes along with the permanent disclosure of sensitive and personal data. Despite the concerns individuals have regarding their information privacy, they act oppositional. However, through the permanent disclosure of sensitive and personal information, privacy of individuals is at risk. The risk of privacy is intensified by the classification of the mobile app download and the usage decision processing as low effort processes without much deliberation. Therefore, the article follows the call of Dinev et al. (2015) to consider principles from behavioural economics and social psychology to investigate its influences on privacy decisions. This is operationalised with six independent experiments to examine the influence of cognitive biases on app information privacy concerns. The results support the underlying assumption of app decision-making as a low effort process and confirmed that different stimuli do influence privacy concerns of individuals. This research contributes to the increasing importance of understanding individuals' behaviour in digital ecosystems.

Keywords: Information Privacy, App Information Privacy Concerns, Low Effort Process, Experiment Series.

1 Introduction

With the mass adoption of personal computers, notebooks, and predominantly smart mobile devices (SMD) like smartphones and tablets the average user of information systems (IS) has dramatically changed (Yoo, 2010). Disruptive innovations like the iPhone, the iPad, and software in form of mobile applications (apps), diffused into the everyday life of users. This leads to fundamental changes concerning how users interact with computing devices and systems (Venkatesh et al., 2012).

Apps are integral to the functioning of SMD and are key elements for the interface design and functionality. Therefore, apps can be interpreted as today's archetype example of ubiquitous computing, i.e. the creation of environments saturated with computing and communication capability, integrated with human users (Weiser, 1991). While ubiquitous computing focuses on hardware components, today's apps are the logical consequence of experiential computing (Yoo 2010). Apps are used to perform every kind of task and users benefit while handling their everyday routine. Everyday activities are almost 'naturally' carried out or supported by apps, or as Apple puts it in one of their slogans: "There's an app for that®" (Apple Inc., 2017) – which addresses the broad scope of applications apps are used for.

However, this excessive level of integration does not come without consequences. Individuals' use of apps poses multiple challenges for IS research, especially in the field of privacy and the disclosure of personal data. It is almost impossible to perform everyday activities without revealing personal data. Individuals disclose consciously or unconsciously personal data while e.g. online shopping, communicate with friends and family, online banking, sharing pictures, and many more (Mai, 2016).

Consequently, privacy as digital personal information and highly personalized data collected via apps has a huge economic value. Thus, most apps are traded for privacy because of their valuable data (Acquisti et al., 2015). However, in contrast to most economic exchanges individuals are usually not able to estimate the quality and performance characteristics of the app they download and use, as well as the amount and economic value of privacy and personal data they disclose and pay with (Spiekermann et al., 2015b; Grossklags and Acquisti, 2007; Buck et al., 2017). Nevertheless, research brings to light that individuals are concerned about their privacy and that they are very sensible regarding the collection and use of their personal data (Grossklags and Acquisti, 2007). Economic theory exhibits, that markets which cannot reduce uncertainty come to a standstill (Akerlof, 1970; Hirshleifer, 1973). In app markets the opposite is observable all over the world: in 2016 users downloaded 149.3 billion mobile apps to their connected devices and it is projected to grow to 352.9 billion app downloads in 2021 (Statista, 2017b). Most of them were downloaded without a monetary price tag (Statista, 2017a). Therefore, apps provoke negative externalities for each individual and for the society as a whole (Arrow, 1974).

An emerging stream in IS and privacy research to investigate this perceived disequilibrium is to integrate frameworks and theories from behavioural economics and social psychology. These approaches incorporate the user as human being as a part of the socio-technical IS to get a better understanding of the existing inconsistencies. Following the call of Dinev et al. (2015), who claim for more research considering human beings as users of IS, we provide a behavioural economics approach on privacy, more precisely on app information privacy concerns. In this paper we present a series of six experiments to investigate the following research question:

- Are common known effects from the field of behavioural economics transferable into digital systems to trigger privacy concerns?

To address this research question, the remainder of this article is structured as follows. In the following section relevant work in information privacy research and its relevance regarding apps is presented. More so, we introduce the current state of approaches from behavioural economics in privacy research and outline the enhanced APCO model. In the methodology section the series of six independent online experiments in the observed field are presented. The supposed and literature driven relations between the dependent and independent variables are shortly introduced and the results are presented. Subsequently, the results are interpreted and the limitations are discussed. Finally, a conclusion is provided containing implications and future research.

2 Relevant Work: Information Privacy, Social Psychology and Behavioural Economics

2.1 Relevant Work in Information Privacy Research

Dinev and Hart (2006) stated that privacy "is a highly cherished value, few would argue that absolute privacy is unattainable" (Dinev and Hart 2006, p.61). Since privacy is addressed in many fields of social sciences and in various areas of everyday life, it lacks a holistic definition (Smith et al., 2011; Solove, 2006). Information privacy refers to information that is individually identifiable or describes the private informational spheres of an individual (Smith et al., 2011). In this paper information privacy is defined as the ability to control the acquisition and use of one's personal information (Westin, 1967; Stone et al., 1983). The concept of autonomous and self-determined control over the disclosure of private information is closely related to information and communication technologies and therewith to SMD and apps (Dinev and Hart, 2006). Within the scope of IS, such as SMD and apps, personal information is gathered by personal data. Thus, this article treats personal information and personal data as equal. We will keep the following principle throughout the remainder of this article: we will use the term privacy as a reference to information privacy, which is our immediate focus.

SMD possess a vast number of connected sensors, devices, and functions. In combination with apps, which are the most common digital user interface, SMD are the enabler to merge the broad opportunities given by the connected entities. Due to these functions, the possibilities of gathering personal data are virtually endless. Future prospects in relation to these applications promise even more opportunities to expand data collection and immediate analysis of data. Regarding data quality, recent developments in mobile technology and an ever-increasing digitization of everyday tasks, lead to an unprecedented precision of continuously updated and integrated personal data, which is generated within information systems. Consequently, apps layer everyday activities and lives in a digital way; or how Clarke rephrased it: "Cyberspace is invading private space" (Clarke, 1999).

With the description of personal data as a new asset class, the World Economic Forum (2011) is in line with the argumentation of many researchers (Smith et al., 2011; Spiekermann et al., 2015a). Derived from the perspective of personal data and privacy as a commodity (Bennett, 1995), many researchers conceive privacy as a tradeable good or asset (Spiekermann et al. 2015a). According to this view, privacy is no longer an absolute societal value, but has an economic value, which leads to the possibility of a cost-benefit trade-off calculation made by individuals or a society (Smith et al. 2011). However, many individuals are not aware when, how and why personal data is collected and with whom it is traded (Acquisti and Grossklags, 2008; Vila et al., 2003). Hence, the market of personal data is characterized by incomplete information, ambiguity and uncertainty (Acquisti and Grossklags, 2005).

A lot of research has been undertaken in the field of information privacy from various disciplines, in particular in the field of IS and individuals' online information privacy (Li, 2011; Dinev et al., 2015; Li, 2011). Privacy and its relation with other constructs have therefore been investigated in several studies. Bélanger and Crossler (2011), Li (2011), and Smith et al. (2011) coincidently investigated the vast privacy literature and established three macro models. Central of many empirical research studies on privacy is the construct of privacy concerns (Kokolakis, 2017; Steijn and Vedder, 2015; Chen and Chen, 2015; Gana and Koce, 2016; Keith et al., 2013). As monitoring of personal information is ubiquitous the concerns about information privacy are growing and it has been a major research area since the mid-1990s (Dinev et al. 2015). It is almost impossible to measure privacy itself as it depends more on cognitions and perceptions rather than on rational decision-making. Therefore, almost all empirical privacy studies in social sciences are based on a privacy-related proxy used as a measurement of information privacy (Bélanger and Crossler 2011; Smith et al. 2011; Xu et al. 2012). Although different wordings have been used like attitudes, beliefs and perceptions, the underlying measurements are generally privacy concerns which were developed to empirically measure information privacy. There is no universal definition for privacy concerns. However, in general it refers to the "degree to which an individual perceived a potential for a loss associated with personal information" (Pavlou 2011, p.981).

Furthermore, Smith et al. (2011) and Li (2011) pointed out the importance of the privacy calculus, suggesting that individuals engage in privacy trade-offs between risk and benefits while engaging in decisions regarding their personal information disclosure (Stone and Stone 1990; Culnan and Armstrong 1999; Dinev and Hart 2006). According to the privacy calculus "individuals are assumed to behave in ways that they believe will result in the most favourable net level of outcomes" (Stone and Stone 1990, p.363). Therefore, users are supposed to undertake an anticipatory, rational weighing of risks and benefits and make fully informed decisions when being confronted to disclose personal information (Malhotra et al., 2004; Culnan and Armstrong, 1999) or conduct transactions (Pavlou 2011). This ties in with the view of neoclassical economics where rational consumers disclose personal information to marketers in exchange for certain benefits (e.g. free access to app service, discounts) but keep other information private if they do not expect to receive benefits (Varian 1996).

The two major constructs in information privacy research, privacy concerns and privacy calculus, describe the dominating declaration gap which existing literature exhibits: the so-called privacy paradox. While most individuals are concerned about their information privacy, they do not act in equal manner. The same individuals are willing to give away their personal information for relatively small rewards (Grossklags and Acquisti, 2007). Following this, individuals show systematic inconsistencies of privacy attitudes and privacy behaviour (Norberg et al., 2007), which are not easily explained by neoclassical models. A promising approach to understand the inconsistencies are existing insights of behavioural economics and decision-making under incomplete information (Kokolakis, 2017; Dinev et al., 2015).

2.2 Privacy and Behavioural Economics in Information Systems

The classic approach of information privacy research supposes that individuals act according to the privacy calculus (Dinev and Hart, 2006; Culnan and Armstrong, 1999; Chellappa and Sin, 2005; Stone and Stone, 1990; Varian, 1996). This is supported by the common definition of privacy concerns which refers to a conscious perception of a potential loss associated with the disclosure of personal information (Pavlou, 2011). This implies that when individuals are confronted with the disclosure of personal information, they deliberately calculate risks and benefits associated with the economic exchange situation (e.g. app versus personal data) (Dinev and Hart, 2006; Culnan and Armstrong, 1999; Chellappa and Sin, 2005). Subsequently, the in the IS research provided and established macro models, which reflect the existing privacy literature, disregard the fact that individuals usually do not fully scrutinize on their behaviour regarding privacy options. So far it is supposed that privacy-related behaviours are represented by deliberate, high-effort processes (Li 2011; Bélanger and Crossler 2011; Smith et al. 2011; Dinev et al. 2015). Thus, all macro models are making the critical assumption that "responses to external stimuli result in deliberate analyses, which lead to fully informed privacy-related attitudes and behaviours" (Dinev et al., 2015). However, it is questionable if individuals make informed decisions regarding information privacy. While they may be aware of the many benefits of the disclosing of personal data (e.g. free usage of app service), the potential costs (e.g. risk of identity theft, price discrimination) are not that obvious due to information asymmetries and the complexity of the system wrapped up in an user friendly, intuitive interface of an app (Marreiros et al., 2017). Hence, privacy decision-making is dominated by information asymmetries, ambiguity, uncertainties and the problem that implications can only hardly be for seen (Acquisti and Grossklags, 2008). Therefore, individuals have mostly no reference points what implications personal information disclosure could lead to in the future (Buck, 2017). Summarized, the declaration gap of the privacy paradox could be caused by a mislead assumption about the way individuals act in situations with incomplete information.

Taking the everyday life integration of modern IS and experiential computing (Yoo, 2010) into account, the current state of IS research does not incorporate enough knowledge known from social psychology and behavioural economics. However, there is growing evidence in this research field that bounded rationality and various cognitive behavioural biases and heuristics can affect individuals personal information disclosure (Acquisti and Grossklags, 2005; Brandimarte et al., 2012; Baek et al., 2014).

Thus, drawing on principles from behavioural economics and social psychology Dinev et al (2015) proposed the enhanced APCO model, shown in figure 1, which postulates that privacy decision-making is

affected by the cognitive resources individuals have and how much level of effort they dedicate when processing decisions regarding their information privacy. Thus, behaviour-relevant information is evaluated using mental shortcuts based on former experienced habits and routines (Polites and Karahanna, 2013). Therefore, simple heuristics and spontaneous reactions during information processing can lead to suboptimal behaviours that are in contrary to individuals expressed believes and values (Dinev et al. 2015). This is expressed in the enhanced APCO model by influences of extraneous factors, inspired by research findings from social psychology and behavioural economics. Although several researchers contributed valuable research to the field (Acquisti and Grossklags, 2005; Acquisti and Grossklags, 2008; Acquisti et al., 2015; Brandimarte et al., 2012), most of the raised questions of Dinev et al. (2015) are not investigated yet.

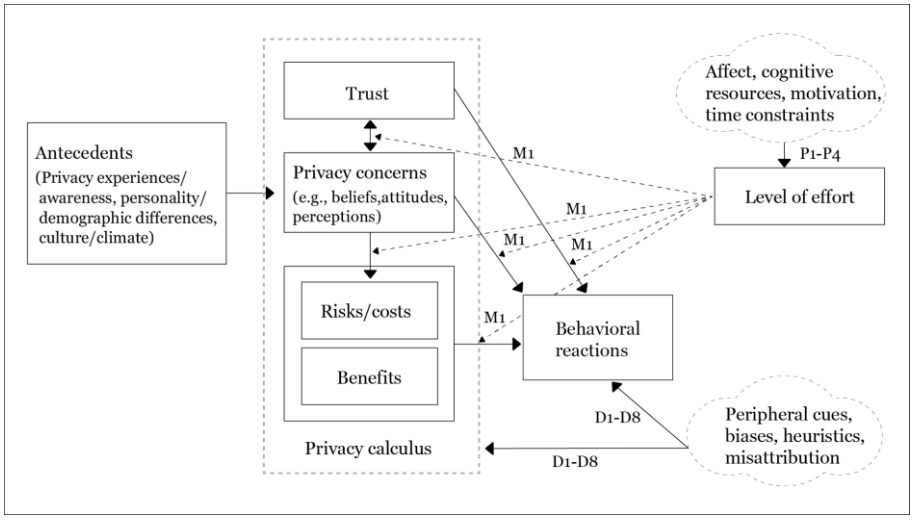

Figure 1. Enhanced APCO-model (Dinev et al. 2015)

Another important variable according to the model is the level of effort (which can range from low-effort up to high-effort processing). It strengthens or weakens the relationship of the variables of the original APCO model, established by (Smith et al., 2011). Low-effort processes are characterized by relatively low cognitive effort or less conscious awareness (Dinev et al., 2015; Kahneman, 2013). We imply that low-effort processes prevail in the app usage and download decision processing due to everyday life integration and the user friendly intuitive interface design. Furthermore, apps are embedded in a complex IS which is difficult to grasp for individuals and due to the information asymmetries it can hardly be retraced.

3 Selection of Cognitive Biases and the Experimental Approach

To make a first attempt to the call from Dinev et al. (2015) we examined common effects known from behavioural economics literature and analysed them regarding transferable mechanisms to influence information privacy concerns. Therewith, we assume a direct influence from extraneous influences (shown in the enhanced APCO-model in the lower cloud) on privacy concerns as a proxy for privacy behaviour.

To investigate the causal relation between possible stimuli and participants' privacy concerns, the app information privacy concern (AIPC) was used as the underlying dependent variable (Buck and Burster, 2017). The construct is based on the central measurements for information privacy concerns in the existing literature. It builds up on the Concern For Information Privacy (CFIP) (Smith et al., 1996), the Internet Users' Information Privacy Concerns (IUIPC) (Malhotra et al., 2004), the Mobile Users' Information Privacy Concerns (MUIPC) (Xu et al., 2012), and the Global Information Privacy Concern (GIPC) of Smith et al. (1996)) and is applied to the context of apps. The AIPC is a one dimensional construct with 17 items and defines to which degree individuals are concerned about their information

privacy regarding mobile apps. In particular, it states *anxiety* which is defined as degree to which a person is concerned about the usage and processing of the collected personal data via mobile apps, *personal attitude* which is related to how important it is for a person to protect their personal data and how sensitive they handle it and *requirements* which is defined as the degree to which an individuals has request towards third parties regarding the handling of their personal data (Buck and Burster, 2017).

To address the research question we conducted a series of six independent experiments using a one factorial-subject design for each experiment. As a result of a discussion with experts in the field we decided to investigate six effects known as *what you see is all there is* (WYSIATI), *prior experience*, *framing*, *scrambled sentences*, *order of information*, and *availability*. The six stimuli are literature driven and have been studied by well-known researchers in social psychology and behavioural economics (Bargh et al., 1996; Schwarz, 1990; Brenner et al., 1996; Kahneman, 2013; Tversky and Kahneman, 1981; Asch, 1946; Nisbett and Wilson, 1977; Tversky and Kahneman, 1973; Srull and Wyer, 1979). The six stimuli were used as an independent variable to examine its effect on AIPC as the dependent variable. In the following we describe the theoretical foundation of the selected effects and outline the operationalisation for the experiments:

The first experiment we developed is based on the effect *what you see is all there is* (WYSIATI) and its research design is shown in figure 2.

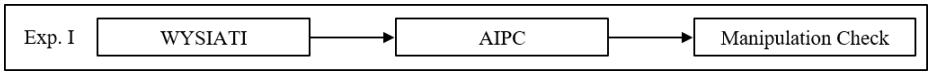

Figure 2. Experiment 1 - Study Design

It is a cognitive bias created by low mental processing as the given information is not questioned or verified by users (Brenner et al., 1996; Kahneman, 2013). Therefore, individuals do not assess the relevance or the quality of the information which leads to a more coherent picture of the situation (Kahneman, 2013). Following this, experiment 1 tries to subconsciously influence the participants with certain information. The stimulus for the treatment group was implemented by displaying a chart to the participants with the reference, that about 75% of all apps have access to at least one of the displayed functions (location, device id, access to other profiles, camera, contacts, list of all calls, microphone, sms, calendar) (Statista, 2014). Due to the displayed information, we hypothesize that the stimulus will lead individuals towards a higher AIPC in comparison to the control group.

Experiment 2 aims to test the influence of prior experience on the AIPC. It focuses on the influence of antecedents in combination of the extraneous factors and their influence on the AIPC (Smith et al. 2011; Dinev et al. 2015). Its research design is shown in figure 3.

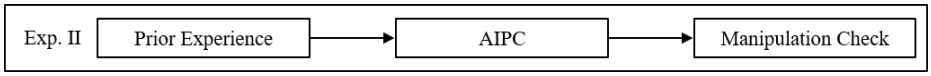

Figure 3. Experiment 2 - Study Design

Research has suggested that prior privacy experience may influence the individual's information privacy concerns (Culnan, 1993; Stone and Stone, 1990). Merely by being exposed to questions about personal prior privacy experience can lead to misattribution effects which are closely related to peripheral cues (Dinev et al., 2015). Those misattribution effects can arise when individuals wrongly ascribe an experience and act upon it with a misunderstanding of the situation (Bem, 1967; Kahneman and Frederick, 2002). To conduct the experiment, the treatment group had to answer several questions about their prior privacy experience, based on the dimensions for prior privacy experience by Xu et al. (2012) (deduced from Smith et al. 1996). We hypothesize that the stimulus will lead individuals towards a higher AIPC because of the misattribution effect on questions about their prior privacy experience. Hypothetically, the participants will overestimate privacy problems, even if they had no negative prior experience.

The third experiment makes use of a scrambled sentence test (Srull and Wyer, 1979; Bargh et al., 1996) to influence individuals' AIPC. Its research design is shown in figure 4.

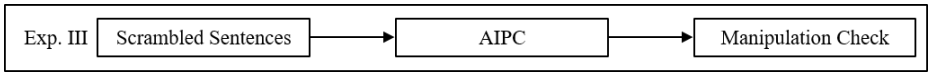

Figure 4. Experiment 3 - Study Design

Bargh et al. (1996) showed with the "Florida-Effect" that actions and emotions can be primed by occasions individuals are not even conscious about. For the experiment the two groups were exposed to a series of 10 scrambled word groupings. The task was to construct a grammatical correct four-word sentence out of a set of five-word elements. The five words for each sentence were displayed in a scrambled order such as "my; privacy; threaten; apps; respect". For the treatment group, it was intended to prime AIPC. Therefore, the sentence contained words related to the topics: personal data, apps, privacy. Each four-word combination could be created with either a positive verb: use, trustworthy, protect etc. or with negative verbs: dubious, share, abuse etc. The control group did also get a scrambled sentence test, however, there was no prime involved. Thus, they got displayed neutral sets of five-word elements in scrambled order such as "I; apple; eating; like; cutting". We hypothesize that participants in the treatment condition have higher AIPC due to the subconscious influence regarding apps compared to the control group.

The fourth experiment is testing a peripheral cue known as framing. Its research design is shown in figure 5.

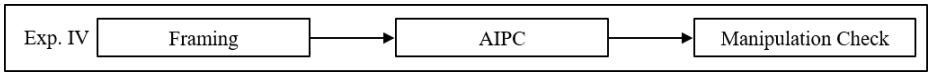

Figure 5. Experiment 4 - Study Design

The effect aims to give the same information framed in a positive and negative formulation (Tversky and Kahneman, 1981; McNeil et al., 1982). Different representations of the same information evoke different emotions and determine how an information is perceived (Goes, 2013). The idea of formulating the same information in two different ways can be transferred to the field of information privacy as IS research has already emphasized the possible influence of message framing on privacy and trust (Angst and Agarwal, 2009; Lowry et al., 2012). Thus, experiment four aims to examine the influence of this framing effect towards AIPC. It was designed with two treatment groups, which got the same pie-chart displayed. The difference between the treatment groups was the formulation of the message beside the pie-chart: "94% of all apps in the App Store are uncritical" vs. "6% of all apps in the App Store are critical" (Bruce Snell, 2016). Before the participants were exposed to the stimulus, they got a description of what we understand critical/uncritical apps are, to ensure all participants will have the same understanding of the term. We hypothesize that the stimulus of treatment group I (negative frame: 6% critical apps) will cause a negative effect leading to a higher AIPC compared to the control group and the treatment group II (positive frame: 94% uncritical apps).

The idea of the fifth experiment is to examine if the halo effect holds for attributes of apps and thus influences the individual's AIPC. Its research design is shown in figure 6.

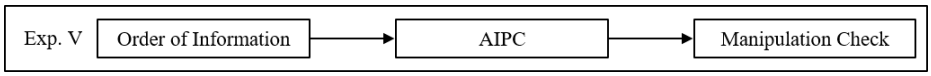

Figure 6. Experiment 5 - Study Design

In theory, the halo effect is a cognitive bias which results in a more coherent picture of people and situations (Asch, 1946; Nisbett and Wilson, 1977). The effect can be described as the tendency to like or dislike all attributes of an object without knowing it in detail and being able to judge all its attributes (Nisbett and Wilson 1977). The order of the sequence of attributes can lead to different impression about the same object, person, or situation because the first attributes in the list override the meaning of the subsequent attributes due to the halo effect (Asch 1946). To set up the experiment, a list of app attributes

was presented in different orders to the two treatment groups. The participants were randomly assigned to one of the three experimental groups. The difference between the two treatment groups was the order (positive to negative) of five given attributes. Treatment group I was exposed to the positive (descending) sequence: very good evaluations; cost-free app; attainment of an aim; function abuse; unauthorized data transfer. Treatment group II was exposed to the list of attributes in the reverse order (negative to positive). We hypothesize that the positive sequence of attributes will cause a positive effect on the AIPC leading to a lower information privacy concern and vice versa to the reversed sequence.

Experiment six aims to prime the influence by naming critical or uncritical apps. Its research design is shown in figure 7.

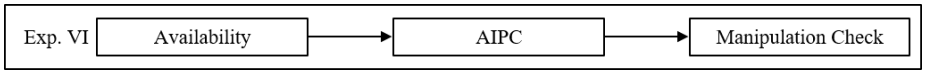

Figure 7. Experiment 6 - Study Design

In situations of uncertainty individuals use simplifying strategies, such as heuristics, to make decisions (Tversky and Kahneman, 1973). The experimental setting is based on the work of Schwarz et al. (1990), who requested subjects to estimate their assertiveness. Participants were asked to describe only few or many examples of being assertive or unassertive (Schwarz, 1990). If the recall process was easy, the subjects judged themselves according to the recalled behaviour. When the recall process was difficult, the corresponding recall affected self-judgement was the opposite to the implications of the recalled behaviour (Schwarz, 1990). Besides a control group, we arranged two main treatments in which participants were asked to name either critical or uncritical apps (free fields; no force to respond). According to Schwarz (1990) we set up two sub-groups (name three or six apps) for each main treatment to test for the implications of the ease or difficulty of recall on the AIPC. Before the participants were exposed to the stimuli, they got a description of what we understand as critical/uncritical apps to ensure all participants will have the same understanding of the term. We hypothesize that individuals are primed by naming critical/uncritical apps. Further we hypothesize that individuals have a lower AIPC if they cannot easily recall any negative experience regarding the usage of personal data by apps. The fluency with which the individuals are recalling examples to judge the frequency of critical apps is relatively low and in consequence they have a lower AIPC. Contrary, if individuals are not able to list uncritical apps their AIPC is rather high. This leads to a bias that is due to the retrieval of examples.

4 Data Collection, Data Set, and Results

The data collection took place from the November 2016 until December 2016. The participants were mostly students from a German university. In each experiment the participants were randomly assigned to either the treatment group(s) or the control group. Overall 1599 individuals participated in the six experiments. 1126 responses were used for analysis. We ensured that there was no overlap of participants in the six experiments. Five experiments were conducted by personally addressing students before their lecture. The (same) experimenter gave a short and always similar introduction about the conducted experiment. Following this, the experimenter encouraged the participants to enter a short-URL to get access to the study with their smartphone. Thus, we aimed to exclude the experimenter bias and ensured independent samples. The sixth experiment was conducted by an anonymous online experiment distributed via social media.

Data collection was conducted via online survey experiment and was set up as follows: the participants got a short introduction and were asked a filter question whether they own or do not own a SMD. If they did not, they skipped automatically to the end of the survey and were excluded from the study as experiences with SMD, and thus with apps, is essential for valid responses (Payne et al., 1999). Subsequently, the prevailing stimulus was applied randomly. As dependent variable, the App Information Privacy Concern (AIPC) was tested immediately afterwards. The 17 items of the AIPC were displayed in randomized order. Subsequently, the participants had to pass an experiment-specific manipulation check

before answering some socio-technical items. Table 1 illustrates the descriptive statistics of the six experiments.

	Experiment 1	**Experiment 2**	**Experiment 3**	**Experiment 4**	**Experiment 5**	**Experiment 6**
n	177	156	205	266	301	494
n (valid resposnses)	147	125	143	207	181	323
n treatment group I	80	58	70	55	41	57
n treatment group II	-	-	-	57	51	55
n control group	67	67	73	95	89	88
M (age); SD (age)	20.00; 1.85	19.90; 1.83	23.34; 3.23	20.44; 2.05	23.28; 3.88	26.07; 6.68
female	57,8% (n=85)	48.8% (n=61)	37.1% (n=53)	58.9% (n=122)	39.2% (n=71)	47.4% (n=153)
male	42.2% (n=62)	51.2% (n=64)	62.9% (n=90)	41.1% (n=85)	60.8% (n=110)	52.6% (n=170)
iOS / non-iOS (n)	83 / 64	68 / 64	66 / 77	96 / 111	81 / 100	163 /160

Table 1. Descriptive Statistics[1]

For experiment 1-3 we followed the classical experimental analysis (Bargh et al. 1996; Tversky and Kahneman 1981; Schwarz 1990). We compared mean values (MV) by t-test of the experimental group (exposed to stimulus) and the control group regarding their overall AIPC and its three dimensions anxiety, personal attitude and requirements. Major results of the experiments are shown in table 2.

The experiment WYSIATI shows that the stimulus, in form of the chart with information on apps, leads to higher concerns on the level of personal attitude. However, this is only confirmed on a gender level for male for the AIPC and personal attitude. For OS-affiliation the stimulus shows significant differences for non-iOS for the AIPC and anxiety.

The second experiment shows that the retrieval of prior experience leads to higher AIPC on an overall level. However, this is only confirmed on a gender level for male for the AIPC, personal attitude and anxiety. For OS-affiliation the effect was confirmed for iOS on the factor personal attitude.

The third experiment reveals that the scrambled sentence exercise leads to higher AIPC. Significant differences for the overall AIPC, personal attitude and anxiety were found. However, this is only confirmed on a gender level for male for the AIPC, personal attitude and anxiety. For OS-affiliation the exercise showed significant differences for iOS for anxiety and for the AIPC and personal attitude for non-iOS.

In experiment 4 to 6 each had at least three different experiment groups. Therefore, we conducted a one-factorial analysis of variance (ANOVA) to test the groups on significant differences regarding their overall AIPC and its three dimensions anxiety, personal attitude and requirements using Gabriel as a Post-Hoc-Test (Field, 2013). There are no significant differences on a 5% level between the experimental groups in the experiments 4-6.

Following the classical experimental analysis (Bargh et al. 1996; Tversky and Kahneman 1981; Schwarz 1990), we also compared mean values by conducting an independent t-test of the two treatment groups (exposed to reversed stimuli).

For experiment 4, the framing effect showed no significant differences neither for gender nor for OS-affiliation.

The fifth experiment shows that order of information leads to higher AIPC and shows significant differences in personal attitude. However, this is only confirmed on a gender level for male for the AIPC. For OS-affiliation the stimulus of experiment one shows significant differences for non-iOS for the AIPC, anxiety and personal attitude.

[1] In experiment 6 we only reference to the positive treatment groups because for the negative treatment groups no significant results were found treatment group III (n= 56) treatment group IV (n=67).

In the sixth experiment we also compared MVs (t-test) of the four treatment groups (critical & uncritical apps). The experiment shows that the heuristic was only confirmed for the different positive treatments (naming three or six uncritical apps) for overall AIPC and anxiety. This is also true for men for overall AIPC. However, for female no significant differences could be found. For OS-affiliation the heuristic was confirmed for non-iOS for the AIPC, as well as anxiety.

		n_1	n_2	AIPC	Anxiety	Personal Attitude	Requirements
WYSIATI	Total	80	67	t(145)=1.577, p=.117,	t(145)=1.096, p=.275	p < 0.05; t(145)=2.051, p=.042	t(145)=.935, p=.352
	Female	47	38	t(83)=.547, p=.586	t(83)=.407, p=.685	t(83)=.490, p=.626	t(83)=.370, p=.713
	Male	33	29	p< 0.1; t(60)=1.689, p=.097	t(60)=1.183, p=.242	p< 0.01 t(60)=2.654, p=.010	t(60)=.958, p=.342
	iOS	45	38	t(81)=.296, p=.768	t(81)=-.243, p=.809	t(81)=1.422 p=.159	t(81)=-.0250, p=.980
	non-iOS	35	29	p< 0.1; t(62)= 1.875 p=.065	p< 0.1; t(62)=1.711, p=.092	t(62)=1.470, p=.146	t(62)=1.441, p=.155
Prior Experience	Total	58	67	p< 0.1; t(123)=1.648, p=.103	t(123)=1.381, p=.170	t(123)=1.553, p=0.123	t(123)=1.182, p=.240
	Female	23	38	t(59)=-.375, p=.709	t(59)=-.401, p=.690	t(59)=-.303, p=.763	t(59)=-.829 p=.411
	Male	35	29	p < 0.05; t(62)=2.353, p=.022	p< 0.1; t(62)=1.920, p=.0590	p < 0.05;t(62)=2.296, p=.025	t(62)=1.620, p=.110
	iOS	27	38	t(63)=1.484, p=.145	t(63)=1.125, p=.267	p< 0.1; t(63)=1.946, p=.056	t(63)=1.350, p=.182
	non-iOS	37	29	t(58)=.994, p=.324	t(58)=.971, p=.336	t(58)=.255, p=.800	t(58)=.768, p=.445
Scrambled Sentences	Total	70	73	p < 0.05; t(141)=-2.247, p=.026	p < 0.05; t(141)=-2.153, p=.033	p< 0.01; t(141)=-3.090, p=.002	t(141)=-.465, p=.642
	Female	26	27	t(51)=-.306, p=.761	t(51)=-.709, p=.482	t(51)=-.457, p=.650	t(51)=.804, p=.425
	Male	44	46	p< 0.01; t(88)=-2.657, p=.009	p < 0.05; t(88)=-2.245, p=.027	p< 0.01; t(88)=-3.461, p=.001	t(88)=-1.159, p=.250
	iOS	34	32	t(64)=-1.183, p=.241	p< 0.1; t(64)=-1.704, p=.093	t(64)=-1.245, p=.218	t(64)=.415, p=.680
	non-iOS	36	41	p < 0.05; t(75)=-2.252, p=.027	t(75)=-1.538, p=.128	p< 0.01; t(75)=-3.540, p=.001	t(75)=-1.393, p=.168
Framing	Total	55	57	t(110)=-.131, p=.896	t(110)=-.335, p=.739	t(110)=.331, p=.742	t(110)=.096, p=.932
	Female	33	33	t(64)=.557, p=.579	t(64)=.044, p=.965	t(64)=1.475, p=.145	t(64)=.387, p=.700
	Male	22	24	t(44)=-.829, p=.412	t(44)=-.619, p=.539	t(44)=-1.252, p=.217	t(44)=-.313, p=.756
	iOS	22	35	t(55)=.539, p=.592	t(55)=.300, p=.765	t(55)=.958, p=.342	t(55)=.210, p=.834
	non-iOS	33	22	t(53)=-0.043, p=.966	t(53)=-.123, p=.903	t(53)=-.093, p=.926	t(53)=.371, p=.712
Order of Information	Total	41	51	p< 0.1; t(90)= -1.662, p=.100	t(90)=-1.352, p=.180	p< 0.1; t(90)=- 1.675, p=.097	t(90)=-1.110, p=.270
	Female	15	21	t(34)=-.612, p=.544	t(34)=-.415, p=.681	t(34)=-.663, p=.512	t(34)=-.415, p=.681
	Male	25	30	p< 0.1; t(53)=-1,778, p=.081	t(53)=-1.495, p=.141	t(53)=-1.609, p=.114	t(53)=-1.088, p=0.282
	iOS	24	25	t(47)=-.614, p=.542	t(47)=-.349, p=.729	t(47)=-.624, p=.536	t(47)=-.748, p=.458
	non-iOS	16	26	p < 0.05; t(40)=-2.170, p=.036	p< 0.1; t(40)=-1.906, p=.064	t(40)=-2.222, p=.320	t(40)=-1.078, p=.288
Availability	Total	57	55	t(110)=-1.466 p=.146,	p< 0.1; t(110)=-1.862, p=.065	t(110)=-1.200, p=.233	t(110)=-0.071, p=.943
	Female	26	31	t(55)=-.553, p=.583	t(55)=-.776, p=.441	t(55)=-.545, p=.588	t(55)=.359, p=.721
	Male	31	24	t(53)=-1.370, p=.176	p< 0.1;t(53)=-1.712, p=.093	t(53)=- 1.008, p=.318	t(53)=-.341, p=.734
	iOS	33	30	t(61)=-.389, p=.699	t(61)=-.467, p=.642	t(61)=-.677, p=.501	t(61)=.387, p=.700
	non-iOS	24	25	p< 0.1; t(47)=-1.788, p=.080	p< 0.1; t(47)=-2.423, p=.019	t(47)=-1.008, p=.319	t(47)=-.504, p=.617

Table 2. Table of Results[2]

5 Interpretation and Limitations

In the introduction we posed the research question: Are common known effects from the field of behavioural economics transferable into digital systems to trigger privacy concerns?

To answer this question, we presented a series of six experiments providing the influence of several stimuli on app information privacy concerns. The results showed that *WYSIATI, prior experience, scrambled sentences, order of information,* and *availability* have a significant influence on app information privacy concerns or sub dimension of the measurement. Although we found significant differences in most experimental settings, not every effect could be transferred into digital systems. Nevertheless, the findings suggest that effects from the fields of behavioural economics and social psychology

[2] Experiment 6 refers to positive treatment groups I & II (naming 3 uncritical versus 6 uncritical apps) because the evaluation of the other treatment groups III & IV (naming 3 critical versus 6 critical apps) did not show significant results.

are fruitful sources to get a better understanding of the decision-making behaviour of users in digital systems.

Generally, the results emphasize the classification of users' behaviour in information systems as low-effort processes with limited cognitive effort. All of the chosen stimuli operationalise an effect which leads to a simplification of the decision-making situation for the users who do not have complete information or are objectively not able to handle the complexity of the underlying IS.

Experiment 1 (WYSIATI) and experiment 5 (Order of Information) show that users constitute their decisions regarding information privacy on the displayed information and its order. According to that, app providers could easily hide critical information containing the high disclosure of personal data by raising the barriers to get in touch with this higher privacy price tags. This is in line with the missing attention of online users when confronted general terms and conditions or online privacy policies (Marreiros et al., 2017). For information privacy theory these findings scrutinise the neoclassical foundation of the existing and dominant macro models in information privacy research. Modern digital systems like current app stores are optimised regarding their usability and the download funnel to satisfy users' needs as fast as possible. This goes in line with the perception-behaviour link and the automatic goal pursuit, known from the domain of consumer behaviour (Dijksterhuis et al., 2005; AARTS and DIJKSTERHUIS, 2000). Accordingly, consumers download or purchase decision is unconscious and highly triggered by the environment. The automatic goal pursuit implies that goal-directed behaviour can be proceeded unconsciously and is only guided by the environment, which in digital systems is fully controlled by the ecosystem provider.

On the other hand, experiment 2 (Prior Experience), experiment 3 (Scrambled Sentences), and experiment 6 (Availability) show that the low-effort processing, which leads to unconscious privacy decisions, can be disturbed. With only tiny exercises users can be triggered to increase their level of effort which leads to more conscious download or purchase decisions.

Both directions of the results show the vulnerability of users regarding nudges in digital systems (Ariely, 2009; Acquisti, 2012). In digital ecosystems like app stores, most of the environment in which users' decisions take place can be controlled by the ecosystem provider. While the providers can misuse this power to lead their users to disclose too much of their personal information, regulation makers could design policies that the low-effort processing of users when downloading and purchasing apps is interrupted.

Experiment 4 (framing) was the only experiment were the stimulus did not influence individual's app information privacy concern. It is very likely, that this is due to a mistake in the experimental design. We suppose that visualisation in form of the pie-chart overshadowed the intended frame of the information.

Moreover, it can be deduced that the personal approach towards personal information does have an important influence on privacy concerns. Looking at the single experiments, the comparison of iOS and non-iOS shows interesting results. Compared to iOS users, non-iOS users seem to be more anxious and concerned when being exposed to a stimulus. This is probably due to the fact that individuals who are using iOS, are feeling more protected within their used ecosystem. Whereas non-iOS users are more often confronted with malicious apps, Apple claims a stricter control process for accredited apps in their AppStore which could lead to a higher trust towards the ecosystem provider. Regarding gender, significant differences could be found. This results are supported by general research on the differences between female and male, which provide evidence for a higher risk aversion of women (Eckel and Grossman, 2008).

Furthermore, the results of the experiments suggest that the enhanced APCO model should be broadened or even rethought. The basic constructs of the model assume a high-effort processing of users when making decisions in digital systems. Regarding the everyday life integration of SMD and apps, the high fragmentation of activities supported by apps and the invisibility modern IS this assumption should be reconsidered. Moreover, the moderating effect of the level of effort on several relations in the APCO model should be reconsidered, too. The results of the experiments suggest that the level of effort has a

direct effect on the second cloud of the model (extraneous influences) or even on the relationships between the cloud and the central constructs (privacy concern, privacy calculus, and trust) or the privacy behaviour.

The experiments are subject to several limitations due to the nature of our research. Firstly, the sample size does not represent all age groups because of the large number of students. Moreover, we did not consider culture bound issues as the sample only consists of German users of SMDs (Krasnova and Veltri, 2010). In addition, we only have very general information on the demographic characteristics of our respondents, which limits the ability to relate app consumers' information seeking behaviour to demographic characteristics. With addressing specific lectures for the data collection, we also limited our validity in terms of a deficit of randomization. An additional limitation lies in the field of application, which also limits the generalizability of the findings for the use of IS. A further limitation is, that we do not know the level of literacy (specific knowledge in the field) the participants had, e.g. regarding the functionality of apps and the processing of personal information. It is possible that with more elucidation and knowledge transfer in the area of digital ecosystems individuals are more conscious and reflecting, when they are disclosing personal information, attended by a higher level of effort. Further, when we asked about critical/uncritical apps in our experiments (four and six), we gave the participants a description of what we understand as critical/uncritical apps to ensure everyone will have the same understanding of the term. However, as there were only slight differences in those experiments it is possible that this was too much information influencing the low-effort process. Additionally, we asked in experiment two participants how often they were exposed to negative privacy incidents. If they did not (consciously) experience privacy abuse, the stimulus could mislead. Further, according to the enhanced APCO model, we did not bear related constructs (e.g. privacy calculus and trust) in mind which could affect the privacy concern and its liability to the exposed stimuli. Due to the fact that we provide a series of experiments with an overview of the results, we did not analyse underlying more in-depth effects of the experiments. As the dependent variable we choose AIPC as our central construct, with which generally intentions were measured. It has been taken into account, that they do not necessary lead to actual behaviours. Moreover, the contextual dependence is an important factor when it comes to information privacy (Smith et al., 2011; Nissenbaum, 2010; Bélanger and Crossler, 2011). Therefore, it is likely that individuals have divergent privacy concerns depending on which apps they use. They might have high concerns regarding health and banking apps but could have lower concerns while using gaming or news apps.

6 Conclusion and Further Research

Our paper deals with the question whether individuals react on exposed stimuli with a change in the app information privacy concern (AIPC). To investigate the research question we conducted six independent experiments with altogether 1599 participants. Even though the results of the experiments were not highly significant in all experimental settings, there is an overall tendency that the chosen stimuli do affect individuals in digital ecosystems. This leads to possible implications for practice and research (Acquisti, 2012). In practice we see app providers and governmental regulation as two sides of the same coin. Whereas app providers could use the results from the experiments to further develop apps in terms of data disclosure, policy-making could start to protect users by intervening and bursting low-effort processing in digital ecosystems. App providers could try to mislead users by e.g. providing optimized orders of information. While policy makers could force app providers to e.g. incorporate questions or tests which arouse attention to the privacy-related action the users want to undertake with the proposed download. This could lead to a governmental action plan by introducing the concept of 'digital nudging'.

The idea is to design IS that offer individuals more informed choices and thus increasing individual and societal welfare by nudging them towards a more sensible handling of their personal data (Acquisti, 2012).

This study was a first attempt to transfer effects and cognitive biases known from behaviour economics and social psychology to the field of IS research. We addressed the call of Dinev et al. (2015) of rethinking the APCO model. Although the experiments represent a low-threshold attempt to the field, the results

of the experiments show the relevance of such investigations to understand users' behaviour in information systems. The paper supports and broadens the propositions of Dinev et al. (2015) that peripheral cues, heuristics, biases, and misattributions do have an impact on information privacy concerns, and subsequently on privacy behaviours.

We approached the complex field of information privacy behaviour of individuals with experimental methods and are aware that no single study can examine the complexity of the enhanced APCO model. However, this study contributes to the field of behavioural economics research and IS and calls for further research to investigate individuals' behaviour in information systems.

Further research should investigate particularly privacy awareness, attitudes, concerns and behaviour in app markets due to the increasing relevance of app usage as the most common user interface to merge smart environments with connected sensors and devices. Moreover, it is important to conduct more research in finding suitable instruments for measuring information privacy concern, especially while conducting experiments. Only with a suitable measurement, conclusions on the causal relationship between the independent and the dependent variable can be drawn. We made an attempt to come up with a reliable and valid measurement, however, it is important to replicate these findings to increase validity (e.g. lab experiment) and to further develop the construct. This is also true for the results of the experiments. To ensure the external validity of the results a replication of the experiments is needed.

So far this paper, makes the assumption that individuals engage one-on-one with app providers and thus does not incorporate the theory of collective action (Olson, 1971; Ostrom, 1990). For further research it might be interesting to investigate how individual's privacy concerns are influenced if there is a third party provider who safely stores and manage personal data of individuals and the account owner decides which personal information to share and with whom (Hafen et al., 2014). Further research should also focus more on the economic theory of social costs which arise because some things do not have a price tag (Ramazzotti, 2012). This is particularly true for personal information. The value of personal data is massive especially in its aggregated form. Therefore, further research should focus on how personal information can be priced that individuals can make more rational choices when disclosing information online.

Moreover, researchers should investigate other factors (antecedence, trust, risk, regulations) of the enhanced APCO model and their linkages with privacy behaviour. Therefore, it might be helpful to not only consider privacy concerns as measurement for privacy behaviour. It is also important to consider other constructs (e.g. attitudes) which are common in marketing and consumer behaviour research.

7 References

AARTS, H. and A. P. DIJKSTERHUIS (2000). "THE AUTOMATIC ACTIVATION OF GOAL-DIRECTED BEHAVIOUR: The case of travel habit." *Journal of Environmental Psychology* 20 (1), 75–82.

Acquisti, A. (2012). "Nudging privacy: The behavioral economics of personal information." In: *Digital Enlightenment Yearbook 2012*, p. 193–197.

Acquisti, A., L. Brandimarte and G. Loewenstein (2015). "Privacy and human behavior in the age of information." *Science (New York, N.Y.)* 347 (6221), 509–514.

Acquisti, A. and J. Grossklags (2005). "Privacy and Rationality in Decision Making." *IEEE Security and Privacy*, 24–30.

Acquisti, A. and J. Grossklags (2008). "What can behavioral economics teach us about privacy." *Digital Privacy: Theory, Technologies, and Practices*, 363–377.

Akerlof, G. A. (1970). "The Market for "Lemons": Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* 84 (3), 488.

Angst, C. M. and R. Agarwal (2009). "Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion." *Management information systems mis quarterly* 33 (2), 339–370.

Apple Inc. (2017). *Apple Trademark List*. URL: http://https://www.apple.com/legal/intellectual-property/trademark/appletmlist.html.

Ariely, D. (2009). *Predictably irrational:* The hidden forces that shape our decisions. Rev. and expanded ed., 3. [print]. New York, NY: Harper Collins Publ.

Arrow, K. J. (1974). "General economic equilibrium: Purpose, analytic techniques, collective choice." *The American Economic Review* 64 (3), 253–272.

Asch, S. E. (1946). "Forming impressions of personalities." *Journal of Abnormal and Social Psychology* (41), 258–290.

Baek, Y. M., E.-m. Kim and Y. Bae (2014). "My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns." *Computers in Human Behavior* 31, 48–56.

Bargh, J. A., M. Chen and L. Burrows (1996). "Automaticity of social behavior: Direct effects of trait construct and stereotype-activation on action." *Journal of Personality and Social Psychology* 71 (2), 230–244.

Bélanger, F. and R. E. Crossler (2011). "Privacy in the Digital Age: A Review of Infomation Privacy Research in Information Systems." *MIS Quarterly* 35 (4), 1017–1041.

Bem, D. J. (1967). "Self-perception: An alternative interpretation of cognitive dissonance phenomena." *Psychological Review* 74 (3), 183–200.

Bennett, C. J. (1995). "The political economy of privacy: a review of the literature." *center for social and legal research, DOE genome project (Final draft), University of Victoria, Department of Political Science, Victoria*.

Brandimarte, L., A. Acquisti and G. Loewenstein (2012). "Misplaced Confidences: Privacy and the Control Paradox." *Social Psychological and Personality Science* 4 (3), 340–347.

Brenner, L. A., D. J. Koehler and A. Tversky (1996). "On the evaluation of one-sided evidence." *Journal of Behavioral Decision Making* 9 (1), 59–70.

Bruce Snell (2016). "Mobile Threat Report: What's on the Horizon for 2016." *Intel Security*, 1–12.

Buck, C. (2017). “Stop Disclosing Personal Data about Your Future Self.” *Americas Conference on Information Systems*, 1–10.

Buck, C. and S. Burster (2017). “App Information Privacy Concerns.” *Americas Conference on Information Systems*, 1–10.

Buck, C., F. Stadler, T. Eymann and K. Suckau (2017). “Privacy as a Part of the Preference Structure of Users App Buying Decision.” *Leimeister, Jan Marco ; Brenner, Walter (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)*, 792–806.

Chellappa, R. K. and R. G. Sin (2005). “Personalization versus privacy: An empirical examination of the online consumer’s dilemma.” *Information Technology and Management* 6 (2-3), 181–202.

Chen, H.-T. and W. Chen (2015). “Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection.” *Cyberpsychology, behavior and social networking* 18 (1), 13–19.

Clarke, R. (1999). “Internet privacy concerns confirm the case for intervention.” *Communications of the ACM* 42 (2), 60–67.

Culnan, M. J. (1993). “"How Did They Get My Name?: ": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use.” *MIS Quarterly* 17 (3), 341.

Culnan, M. J. and P. K. Armstrong (1999). “Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation.” *Organization Science* 10 (1), 104–115.

Dijksterhuis, A., P. K. Smith, R. B. van Baaren and D. H.J. Wigboldus (2005). “The Unconscious Consumer: Effects of Environment on Consumer Behavior.” *Journal of Consumer Psychology* 15 (3), 193–202.

Dinev, T. and P. Hart (2006). “An extended privacy calculus model for e-commerce transactions.” *Psychology & Marketing* 17 (1), 61–80.

Dinev, T., A. R. McConnell and H. J. Smith (2015). “Research Commentary: Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box.” *Information Systems Research* 26 (4), 639–655.

Eckel, C. C. and P. J. Grossman (2008). “Men, women and risk aversion: Experiment evidence.” In: *Handbook of experimental economics results*. Amsterdam [u.a.]: North-Holland, p. 1061–1073.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics:* And sex and drugs and rock 'n' roll. 4th edition. Los Angeles, London, New Delhi: Sage.

Gana, M. A. and H. D. Koce (2016). “Mobile Marketing: The Influence of Trust and Privacy Concerns on Consumers’ Purchase Intention.” *International Journal of Marketing Studies* 8 (2), 121.

Goes, P. B. (2013). “Editor’s ’ Comments Information Systems Research and Behavioral Economics.” *MIS Quarterly* 37 (3).

Grossklags, J. and A. Acquisti (2007). “When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information.” *Information Security*, 7–8.

Hafen, E., D. Kossmann and A. Brand (2014). “Health data cooperatives - citizen empowerment.” *Methods of information in medicine* 53 (2), 82–86.

Hirshleifer, J. (1973). “Where are we in the theory of information?” *The American Economic Review* 63 (2), 31–39.

Kahneman, D. (2013). *Thinking, fast and slow*. 1. paperback ed. New York: Farrar Straus and Giroux.

Kahneman, D. and S. Frederick (2002). "Representativeness Revisited: Attribute Substitution in Intuitive Judgment." In: *Heuristics and biases: The psychology of intuitive judgement*. Ed. by T. Gilovich, D. W. Griffin and D. Kahneman. Cambridge, U.K., New York: Cambridge University Press, p. 49–81.

Keith, M. J., S. C. Thompson, J. Hale, P. B. Lowry and C. Greer (2013). "Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior." *International Journal of Human Computer Studies* 71 (12), 1163–1173.

Kokolakis, S. (2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon." *Computers & Security* 64, 122–134.

Krasnova, H. and N. F. Veltri (2010). "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA." In: *43rd Hawaii International Conference on System Sciences (HICSS), 2010 ; Honolulu, Hawaii, 5 - 8 Jan. 2010*. Ed. by R. H. Sprague. Piscataway, NJ: IEEE, p. 1–10.

Li, Y. (2011). "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework." *Communications of the Association for Information Systems* 28, 453–496.

Lowry, P. B., G. Moody, A. Vance, M. Jensen, J. Jenkins and T. Wells (2012). "Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers." *Journal of the American Society for Information Science and Technology* 63 (4), 755–776.

Mai, J.-E. (2016). "Big data privacy: The datafication of personal information." *Information Society* 32 (3), 192–199.

Malhotra, N. K., S. S. Kim, J. Agarwal, G. Tech and W. Peachtree (2004). "Internet Users ' The Information the Scale and a Causal (IUIPC)." *Psychology & Marketing* 15 (4), 336–355.

Marreiros, H., M. Tonin, M. Vlassopoulos and M. C. Schraefel (2017). ""Now that you mention it": A survey experiment on information, inattention and online privacy." *Journal of Economic Behavior & Organization* 140, 1–17.

McNeil, B. J., S. G. Pauker, H. C. Sox and A. Tversky (1982). "On the elicitation of preferences for alternative therapies." *New England Journal of Medicine* 306 (21), 1259–1262.

Nisbett, R. E. and T. D. Wilson (1977). "The Halo Effect: Evidence for Unconscious Alteration of Judgments." *Journal of Personality and Social Psychology* 35 (4), 250–256.

Nissenbaum, H. F. (2010). *Privacy in context:* Technology, policy, and the integrity of social life. Stanford, California: Stanford Law Books an imprit of Standford University Press.

Norberg, P. A., D. R. Horne and D. A. Horne (2007). "The Privacy Paradox: Personal Information Disclosure Intentions vers us Behaviors." *The Journal of Consumer Affairs* 41 (1), 100–126.

Olson, M. (1971). *The logic of collective action:* Public goods and the theory of groups. Cambridge, Mass.: Harvard Univ. Press.

Ostrom, E. (1990). *Governing the commons:* The evolution of institutions for collective action. Cambridge: Cambridge Univ. Press.

Pavlou, P. A. (2011). "State of the information privacy literature: Where are we now and where should we go?" *Management information systems mis quarterly* 35 (4), 977–988.

Payne, J. W., J. R. Bettman and D. A. Schkade (1999). "Measuring Constructed Preferences: Towards a Building Code." *Journal of Risk & Uncertainty* 19 (1-3), 243–270.

Polites, G. L. and E. Karahanna (2013). "The embeddedness of information systems habits in organizational and individual level routines: Development and disruption." *Management information systems mis quarterly* 37 (1), 221–246.

Ramazzotti, P. (2012). "Social costs and normative economics." In: *Social costs today: Institutional analyses of the present crises*. Ed. by P. Ramazzotti, P. Frigato and W. Elsner. London: Routledge, p. 15–34.

Schwarz, N. (1990). *Ease of retrieval as information:* Another look at the availability heuristic. Mannheim: ZUMA.

Smith, H. J., T. Dinev and H. Xu (2011). "Information Privacy Research: An Interdisciplonary Review." *MIS Quarterly* 35 (4), 989–1016.

Smith, H. J., S. J. Milberg and S. J. Burke (1996). "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." *Management Information Systems Quarterly* 20 (2), 167.

Solove, D. J. (2006). "A taxonomy of privacy." *University of Pennsylvania Law Review* 154 (3), 477–560.

Spiekermann, S., A. Acquisti, R. Böhme and K.-L. Hui (2015a). "The challenges of personal data markets and privacy." *Electronic Markets* 25 (2), 161–167.

Spiekermann, S., R. Böhme, A. Acquisti and K.-L. Hui (2015b). "Personal Data Markets." *Electronic Markets* (25), 91–93.

Srull, T. K. and R. S. Wyer (1979). "The role of category accessibility in the interpretation of information about persons: Some determinants and implications." *Journal of Personality and Social Psychology* 37 (10), 1660–1672.

Statista (2014). *Mobile Sicherheit: Apps greifen auf sensible Daten zu:* 3/4 aller Apps können auf sensible Funktionen zugreifen. URL: https://www.securepim.com/mobile-sicherheit-34-aller-apps-koennen-auf-sensible-funktionen-zugreifen/ (visited on 12/03/2016).

Statista (2017a). *Number of free mobile app downloads worldwide from 2012 to 2017 (in billions)*. URL: https://www.statista.com/statistics/241587/number-of-free-mobile-app-downloads-worldwide/.

Statista (2017b). *Number of mobile app downloads worldwide in 2016, 2017 and 2021 (in billions)*. URL: https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/.

Steijn, W. M. P. and A. Vedder (2015). "Privacy concerns, dead or misunderstood? the perceptions of privacy amongst the young and old." *Information Polity* 20 (4), 299–311.

Stone, E. F., H. G. Gueutal, D. G. Gradner and S. McClure (1983). "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations."

Stone, E. F. and D. L. Stone (1990). "Privacy in organizations: Theoretical issues, research findings, and protection mechanisms." *Personnel and Human Resources Management,* 8 (3), 349-411.

Tversky, A. and D. Kahneman (1973). "Availability: A heuristic for judging frequency and probability." *Cognitive Psychology* 5 (2), 207–232.

Tversky, A. and D. Kahneman (1981). "The framing of decisions and the psychology of choice." *Science* 211 (4481), 453–458.

Varian, H. (1996). "Economic aspects of personal privacy." *Topics in Regulatory Economics and Policy* (3), 1–12.

Venkatesh, V., J. Y. L. Thong and X. Xu (2012). "Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology." *MIS Quarterly* 36 (1), 157–178.

Vila, T., R. Greenstadt and D. Molnar (2003). "Why We Can't Be Bothered to Read Privacy Policies." *Working Paper*, 143–153.

Weiser, M. (1991). "The computer for the 21st century." *Scientific american* 265 (3), 94–104.

Westin, A. F. (1967). "Privacy and freedom." 25 (1).

World Economic Forum (2011). *Personal Data: The Emergence of a New Asset Class*. URL: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

Xu, H., S. Gupta, M. Rosson and J. Carroll (2012). "Measuring Mobile Users' Concerns for Information Privacy." *ICIS 2012 Proceedings*.

Yoo, Y. (2010). "Computing in everyday life: a call for research on experiential computing." *MIS Quarterly* 34 (2), 213–231.